

IN THE SPECIFICATION

Please amend the paragraph spanning page 6, line 13- page 7, line 19, as follows:

A1

In the present state of the art, computer systems that are properly configured for providing protection against computer viruses, typically permit the opening and closing of files using the steps shown in the flowchart of Figure 2. A user of a personal computer 8 or laptop computer 10, as shown in Figure 1, can request the server computer 4 to open a file for write access, as indicated by step 22. Please note that although various embodiments of the present invention are described in association with a computer network, such as the Ethernet 2 of Figure 1, the invention is not so limited, and can be implemented through use of any other known network. Also, various embodiments of the present invention are applicable for use by a user directly on their own dedicated personal computer 8 or laptop 10. For these and other computer configurations, it is typical after a file is opened for write access in step 22, to next scan the file for viruses in step 24, via a computer anti-virus program. If no viruses are detected in step 24, step 26 is entered for providing the requested file to the Application program of the user. A period of time after the file is opened, it is typical that a user will request that the file be closed. Upon a file closure request being made in step 28, the typical anti-virus program loaded into a computer system, such as network server computer 4, interfaces with the network operating system 6 to scan the file for viruses in step 30 before permitting the file to be written back into memory. As shown in decision step 32, if a file is found to be infected with a virus, the anti-virus program proceeds to step 34 for preventing the infected file from being written into memory, such as file storage memory 18. Alternatively, if in step 32 no virus is uncovered, the anti-virus program proceeds to step 36 for allowing the operating system to write the file back into memory. The last step 38, indicative that scanning has been completed, terminates the typical virus protection program scanning routine. Note that in some state-of-art operating systems, the cache buffers 20 are used to store files upon opening in an unmodified state. Before step 36, the file to be closed is compared to the corresponding unmodified file in a-cache buffers 20-memory ~~30~~. If the file to be closed is found to be identical to the unmodified cached file, write step 36 is skipped, and the open file is closed with only the file's time stamp being updated. In

computers not loaded with an anti-virus program, the file comparison occurs after step 28.

---

A1